2021年度 秋学期

# 卒　業　論　文

# 公的個人認証サービスを利用したデジタル遺品相続手法の提案


指導教員: 上原 哲太郎

立命館大学 情報理工学部

卒業研究3 (BA)

コース: セキュリティネットワーク

学生証番号: 2600180054-9

氏名: 太田 晃

## 概要

様々なサービスがインターネットを通して利用することができるようになっている現在，デジタル遺品と呼ばれる個人が生前に利用していたデジタル機器に保存されたデータやインターネット上での登録情報の処理に対して，様々な問題が生じている．自身の死後のために財産処置の方法を残す手段として遺言書が存在するが，電子的な遺言書や電子的に相続を行うことのできる方法は存在していない．その理由として，遺言書のデジタル化に伴う問題や個人の認証の問題が挙げられる．一般的な遺言書は民法上で，遺言者による「自筆」が要件になっており，スキャナで電子化してもデータの特性上，第三者の検証による遺言書の真正性の証明が難しいことがある．また，相続という重要な出来事において相続人であることを証明することは非常に重要なことであり強固な認証が必要となる．そこで本論文では，電子的な相続を実行するための要件を考察し，既存の制度の活用方法と新たなシステムの導入により電子的相続を実行するための仕組みを考案する．

# 目 次

# 第1章　研究背景

近年，デジタル遺品についての問題がしばしば注目されるようになった．デジタル遺品とは，パソコンやスマホなどのデジタル機器内に保存されているデータ，また，インターネットを通じて利用していたSNSでのやりとりや暗号資産などの各種サービスに関するデータである．遺族はデジタル遺品をどのように入手しどのように処理すべきなのかという問題に直面する場面が多くなった．

総務省の「令和2年通信利用動向調査」[1]によると，個人のインターネット利用率が全体で80%を越えており，年齢別にみても6歳から69歳までの各年齢層で80%を越えているなど，幅広い年齢層でインターネットが利用されていることが分かる．また，SNS利用率は全体で70%を越えている．多くの個人に利用されているデジタル機器の中には，暗号資産の保有情報や他人に見られると恥ずかしい趣味のデータなど，様々なデータが存在しているため，デジタル遺品に関するトラブルが起きる可能性は十分に高いと考えられる．現在，個人のインターネット利用率やSNS利用率においては，高齢者の割合が約50%である．しかし，今後さらに利用割合が増加することが推測される．ここで，利用者が死亡した場合，それまで利用者が使用していたインターネットサービスのアカウントが長期間放置されたままの状態になってしまう．また,「令和2年通信利用動向調査」[1]によると，SNSの利用目的として約90%が「従来からの知人とのコミュニケーションのため」と回答しているように，今やSNSはコミュニケーションのためのツールとして利用することが一般的であり，実際に会ったことはないがSNS上だけでつながっている友人がいるという人も少なくない．遺族が不快な思いをしないためにも，遺族は利用者が亡くなったことを知らせたり，生前にどのようなつながりがあったのかを調べるために遺族が故人のSNSアカウントを利用することは有用である．しかし，利用者が亡くなると，たとえ遺族であってもそのアカウントを操作して何らかの情報を得るということは困難である．実際，主要なSNSの1つである「Twitter」では，ユーザが亡くなった場合は故人との関係を証明したうえで権限のある遺産管理人または故人の家族とともにアカウントを停止，削除することはできるが，故人のアカウントのログイン情報の開示やそのアカウントを操作するといったことは，故人との関係によらず行うことができないとされている[2].

また，その他のサービス，特にFX取引や有料会員サービスなどの金銭に関連するサービスのアカウントが放置され，遺族に追加請求されるというリスクがある．さらに暗号資産に注目してみると放置による知らないうちに発生する被害だけでなく，相続をするときに被相続人が暗号資産を保持していたことが確認できても秘密鍵や秘密鍵を含むパスワードを知らなかった場合，実際にはその暗号資産の送金処理を行うことができないにも関わらず相続税は課税されてしまう．秘密鍵などに関して「知らない」「忘れた」ということを証明することができないからである．これらの問題を引き起こさないようにするために生前に相続人となりうる人物に周知してもらうことや死後どのようにそれらを処理すべきかといった「遺言」が重要になってくる．

「自筆証書遺言書保管制度」という，法務局によって自筆遺言書を管理・保管してくれるサービスがはじめられた[3]．しかし，電子的な遺言書を残し，オンライン上で相続をすることができる仕組みは存在していない．これには，電子的な遺言書が認められていないことや被相続人の死亡確認及び相続人の本人確認をオンライン上で行う仕組みが利用されていないことが関係している．

遺言書民法において本文全体，氏名及び日付を自筆し，押印しなければならなくワープロなどにより電子的に作成された遺言書は有効としないとされている．これは筆跡や氏名をもとに遺言書作成者を特定するためである．

つまり，遺言書の作成者を特定することが可能であるならば電子的な遺言書でも効力を認められてもよいのではないかと考える．そこで，本論文ではオンライン上での相続に必要な仕組み，制度を考察し，それをもとにどのようなシステムであれば電子的な相続として成立するのかということを考案する．

本研究の構成は次の通りである．まず，第 2 章で本研究に関連する技術を説明する．次に，第 3 章で問題解決のために利用できる技術・制度と既存のものでは解決できない問題について示す．さらに，4 章で本研究での提案について説明し，5 章で本提案手法を実装や評価について述べる．最後に，6 章で本研究のまとめと課題，今後の展望について述べる．

# 第2章　関連技術

## 2.1　デジタル遺品

デジタル遺品とは，持ち主が亡くなり遺品となったデジタル機器に保存されたデータやインターネット上の登録情報のことである．具体例として，パソコンやスマートフォンなどのハードウェアに記録されている写真や文章，ウェブサイト上で記録されているメールや SNS アカウント，動画や音楽などの有料サービスのアカウントや暗号資産取引に使用されるアドレスなどが挙げられる．

## 2.2　デジタル遺品の問題点

通常，遺品の相続人は，機器内に残されたデータや機器を元に相続するものや連絡のための交友関係の把握のために手がかりを探し始める．しかし，機器内には多くの情報が蓄積されているため，機器が複数の相続人による共有の状態になる．ある相続人が機器を扱うには，他の相続人の了解をとる必要があるなど手間がかかる．ただ，多くの場合において相続人は，機器へのログイン情報が分からず，デジタル機器そのものへのアクセスをすることができない．そこで，デジタル機器のロックを解除するためにパスワードの解析を行ってくれる業者にお願いして，機器のロックを解除しようとする．しかし，パスワードの解析が必ず成功するわけではない．仮にパスワードが判明，もしくは事前に知っていて機器のロックを解除することに成功し，その機器で故人がどのようなサービスを利用していたかを知ることができたとしても，そのサービスで利用していたアカウントへのログインのための情報までは分からない．また，どのようなやり取りが行われていたのか，どのようなデータが管理されていたかを知ることは非常に難しい．故人が利用していたサービスが判明すれば，そのサービスの運営サイトを訪れ，相続の手続きを行うことができるかもしれない．しかし，運営サイトによる相続手続きを行うためには多くの場合，正当な相続人であることを証明する必要があり，その証明ために死亡証明書や戸籍情報などの紙媒体の情報を郵送するなど手続きが煩雑化している．また，SNS を含めた多くのサービスは基本的にアカウント自体の相続を利用規約により禁止している場合が多く，正当な相続人であっても利用規約違反になることがあるなど規制が多い．

## 2.3　相続

相続とは，故人である被相続人の財産を特定の人物に引き継ぐことであり，被相続人が亡くなったときに発生するものである．相続は，被相続人によって書かれた遺言書があれば原則はその遺言書に沿って行われる．遺言書がない場合は民法で定められている割合に応じて相続を行う法定相続となるか，相続人全員による遺産の分割協議によって財産を分ける場合が存在する．

遺産を受け継ぐ人物は，民法で定められている順位に応じて決定される法定相続人と遺言書で指定された受遺者である．被相続人に配偶者がいる場合，配偶者は常に法定相続人となり，その他は直系卑属，直系尊属，兄弟姉妹の順で法定相続人となる可能性がある．直系卑属とは被相続人の子供またはその代襲相続人である．直系尊属

とは被相続人の父母や祖父母である．第一順位の人物である直系卑属がいない場合にのみ第二順位である直系尊属が法定相続人となるといったように，順位が上の人物がいない場合は，その次の順位の人物が法定相続人となる．図 2.1 に被相続人との関係図を示す．

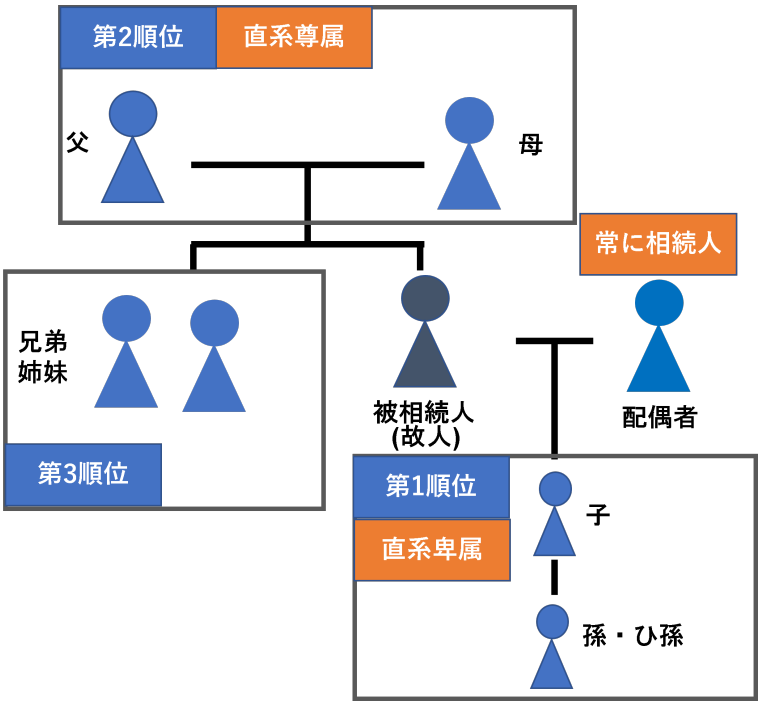


図 2.1: 被相続人との関係.

相続の対象となる遺産には，現金や有価証券，車や土地，権利など有形無形の相続人にとって利益になるものだけでなく，借金や債務といった損失をともなうものもある．しかし，相続人が必ず全ての遺産を相続しなければならないわけでなく，相続を放棄することや相続人全員の同意がいるが，債務の支払いの結果利益になる範囲にとどめるような相続をすることもできる．

## 2.4　相続の遺留分

相続が発生した際，相続人が必ず相続できる最低限の遺産の割合が存在する．それが遺留分である．たとえ遺言によって財産の相続先をどのように指定されたとしても，遺留分侵害額請求を行うことにより，相続人は遺留分を相続することができる．しかし，遺留分侵害額請求できる権利を持つ相続人は，図 2.1 における兄弟姉妹を除いた人物のうち相続人となった人物のみである．請求できる遺留分の割合は民法第 1042 条により，兄弟姉妹以外の相続人において，相続人が直系尊属のみの場合は 1/3，それ以外の場合は 1/2 と定められている．また，相続人が複数人ある場合には，各自の相続分を乗した割合とすると定められている．相続財産全体を 1 としたときの相続人と遺留分の関係を表 2.1 に示す．

相続財産全体を 300 万円としたときの具体例を以下に挙げる．

- 相続人が配偶者と子供 3 人，計 4 人のとき
  配偶者の遺留分は 75 万円，子供の遺留分は 1 人当たり 25 万円となる．

表 2.1: 相続人と遺留分の関係.

| 相続人 | 遺留分全体 | 個人の最終取得割合 |
|---|---|---|
| 配偶者のみ | 1/2 | 配偶者が総どり |
| 配偶者と子供 | 1/2 | 配偶者：1/4， 子供：1/4 (子供が複数人いるときは等分) |
| 配偶者と父母 | 1/2 | 配偶者：1/3， 父母：1/6 (父母が両方いる場合はそれぞれ 1/12) |
| 配偶者と兄弟姉妹 | 1/2 | 配偶者が総どり， 兄弟姉妹に遺留分はない |
| 子供 | 1/2 | 等分 |
| 父母 | 1/3 | 等分 |
| 兄弟姉妹 | なし | なし |

- 相続人が配偶者と兄弟姉妹のとき
  配偶者の遺留分は 150 万円，兄弟姉妹は 0 円となる．

## 2.5 遺言書

普通方式遺言書には，大きく分けて「自筆証書遺言」,「公正証書遺言」,「秘密証書遺言」の 3 種類があり，本論文で注目すべきものは,「自筆証書遺言」である．2020 年 7 月 10 日に法務局による遺言書の預かりサービスとして「自筆証書遺言書保管制度」が開始された．しかし，この制度で預かりが可能なのは「自筆証書遺言」であり，その名の通り「自筆」であることが重要視されている．民法第 968 条 1 項により「自筆証書によって遺言をするには，遺言者が，その全文，日付及び氏名を自書し，これに印を押さなければならない.」と記されている．しかし，2019 年 1 月 13 日に施行された民法第 968 条の改正により，遺言書の財産目録についてはワープロ等の作成が認められ自筆である必要がなくなったが，依然として遺言書の本文は自筆しなければならない．自筆が重要視されている理由は，遺言は，相続をめぐるトラブルを防止するために有用な手段である．特に自筆証書遺言は自筆さえできれば遺言者本人のみで作成が可能であり，証人が不要であるなど低コストで手軽に作成することができる．しかし，遺言書の変造や偽造がなされる可能性が高く，それらが疑われたときに本当に遺言者が作成したものであるかどうかを遺言者の筆跡を元に鑑定するためである．

また，民法第 968 条第 1 項に「自筆証書によって遺言をするには，遺言者が，その全文，日付及び氏名を自書し，これに印を押さなければならない.」とある．日付の記載は，遺言書が複数発見された場合，どちらがより後に作成されたものであるかの判断を可能にし，その日付における遺言者の遺言能力の有無を判断するために利用される．遺言書に署名する氏名としては，遺言者の特定のために原則として戸籍上の本名を書かなければならないが，芸名やペンネームなどの本名以外の記載であっても「遺言者」を特定できるのであれば有効な氏名とみなしてもよいということが記されている [4]．遺言書に押す「印」については，特別な定めが存在しないため実印である必要がなく，指印でも有効性が認められる場合 [5] が存在する．しかし,「指印」による押印や押印の代わりに「花押」を書くことでは民法 968 条の要件を満たさないとして有効性が認められない場合 [6][7] も存在する．これらの有効になった事例と無効になった事例に共通している判決理由の元になっているのは，自筆による遺言書の方式に自書のほかに押印を必要としたのは，遺言の全文の自書と押印によって遺言者の同一性や真正性を確保するとともに，重要な文書は作成者による署名と押印をすることで文書の作成を完結させるということが通例であり，法に照らし合わせても文書の完成を担保するものである，という考えである．つまり，遺言者本人が正式に作成したものであることを確認することが出来るなら有効となり，確認することができないのならば無効になることが分かる．

## 2.6　公開鍵暗号

本稿での公開鍵暗号とは公的個人認証サービスにおいて用いられている暗号方式である RSA 暗号のことを指すものとする．公開鍵暗号では，公開鍵と秘密鍵の 2 つの鍵を 1 組のペアとして扱う．一方の鍵でメッセージの暗号化を行うと，他方の鍵でのみ復号可能である．公開鍵は他者に知られることを前提にしているのに対し，秘密鍵は絶対に他者に知られてはいないことを前提としている．公開鍵からは秘密鍵を作成できないのに対して，秘密鍵から公開鍵を作成することができ，一般に利用する際には，公開鍵で暗号文を復号するためにはそれに対応した秘密鍵を用いるためである．暗号文が第三者に入手されたとしてもその公開鍵に対応する秘密鍵を知らなければその暗号文を解読することができず，メッセージの漏洩を防ぐことができる．

## 2.7　電子署名

電子署名及び認証業務に関する法律 (電子署名法) では同一の法的拘束力が認められているものとして電子サインと電子署名がある．電子サインはタッチペンなどを用いて電子的にサインするものであり，手軽に利用できるものであり，対面であれば目の前にいる相手が契約書にサインする人物であるということが判断できるため有用である．しかし，対面でなければ実際に電子サインをした人物と本来の契約者が同一の人物であるということを電子サインから判別することは困難であるため，対面でないサービスでの本人確認に利用するには信頼性が低い．

電子署名は，紙文書へのサイン，押印といった真正性の証明を電子文書上で実現するための技術である．電子署名を電子文書に付与することにより，文書の改ざんやなりすましを検出することができ，その文書が原本であることが証明できる．電子署名を付与するためには，公開鍵暗号を利用する．文書の送信者は，自身の秘密鍵を用いて文書に署名を施す．受信者は，受け取った文書が本当に送信者によって署名されたものであるかを送信者の公開鍵を用いて検証する．検証に成功すればその文書は真に送信者が作成したものであり，署名付与以降に改ざんされていないことが確認できる．

## 2.8　電子証明書

電子署名が施された文書の署名検証を行うとき，送信者の公開鍵を用いるが，公開鍵が本当に送信者のものであるという証明が必要である．この証明のために電子証明書が必要となる．電子証明書を信頼するべきか否かを判断する規準として，電子証明書にはその電子証明書の発行者や有効期間，公開鍵の所有者の情報などが記載されており，信頼できる第三者 (認証局) によって電子署名がなされている．認証局とは，認証業務運用規定やプライバシーポリシーなどを公開し，信用できることを公に認められている機関であり，公的個人認証サービスにおいては，地方公共団体情報システム機構が認証局の役割を務めている．

## 2.9　公的個人認証サービス

公的個人認証サービスとは，オンラインでの申請や届け出といった行政手続きやインターネットサイトへのログインを行う際に用いられる本人確認の手段である．本人確認には，マイナンバーカードに搭載されている電子証明書を利用する．マイナンバーカードに搭載される電子証明書は地方公共団体情報システム機構により発行されており，マイナンバーカードは耐タンパー性を有しているため，マイナンバーカード内の情報が不正に読みだされたり解析されようとした場合，その内容が自動的に消去されるという対抗措置が講じられている．マイナン

バーカードに搭載されている電子証明書を読み取ることで，電子署名やユーザ認証を行うことができる．公的個人認証サービスは，マイナンバー制度が開始される以前，2004 年 1 月 29 日に個人向けのサービスとして電子証明書の発行が開始されたが，これは，オンラインで行政機関への届け出などを行った人物が本当に住民基本台帳に記録されている人物であるかを確認する仕組みであり，住民基本台帳ネットワークシステムとして存在していた．このシステムでの公的個人認証サービスを利用するためには，住所地市町村に申請して住民基本台帳カードを交付してもらい，その IC チップに電子証明書と秘密鍵を格納する必要があった．以前の公的個人認証サービスによる電子証明書や電子署名の利用は，行政手続きをオンラインで行う場合にのみ利用可能であった．しかし，2013 年 5 月 31 日に公布された社会保障・税番号制度関連四法によって，公的個人認証法の一部が改正 [8] され，公的個人認証サービスの利用範囲が変更された．電子証明書の発行者が都道府県知事から地方公共団体情報システム機構に変更され,「利用者証明用電子証明書」という電子証明書の新設がなされた．さらに，全国民に個人番号が付番されることとなり，2016 年 1 月から住民基本台帳に記録されている者に対し，その者の申請により，個人番号カードが交付されるようになりそれに伴い，住民基本台帳カードの発行が終了するため，電子証明書格納媒体が住民基本台帳カードからマイナンバーカードに変更された．加えて，民間事業者においても電子署名や電子証明書による本人確認サービスが利用可能になった．この業務のことを特定認証業務といい，2016 年 1 月より，総務大臣による認定を受けた民間企業は総務大臣認定事業者となりマイナンバーカードの電子証明書の署名検証・利用者証明検証業務を行うことが可能になった．2022 年 1 月時点での総務大臣認定事業者は 17 社である [9]．

### 2.9.1 公的個人認証サービスにおける電子証明書

現在の公的個人認証サービスでは，二種類の電子証明書が標準で提供されている．署名用電子証明書と利用者証明用電子証明書の 2 つである．署名用電子証明書と利用者証明用電子証明書の違いは，その利用用途と個人情報の基本となる氏名，性別，住所，生年月日の 4 つの情報である基本四情報の記載があるか否か，そして発行・失効条件である．これらの証明書の使用用途は以下の通りである．

- 署名用電子証明書
  電子文書を行政機関に提出するための署名や捺印に相当するものとして署名用電子証明書を利用して電子申請を行う．具体的には，e-Tax の電子申請を行うために利用される．電子文書を作成・送信した者が利用者本人であり，文書が改ざんされていないことを確認するために用いられる．IC カードの紛失をしたために電子証明書の失効申請をしたり，有効期間が満了したり本人が死亡した場合に加えて，住民票の基本四情報の記載が修正された場合に失効する．基本四情報が記載されている．

- 利用者証明用電子証明書
  インターネット上のサービスを利用する際に利用しているのが本人であることを証明するための手段として用いられる．具体的には，マイナポータルへのログインやコンビニでの住民票の交付などの公的な証明書の交付サービスのために用いられる．IC カードの紛失をしたために電子証明書の失効申請をしたり，有効期間が満了したり本人が死亡した場合に失効する．基本四情報は記載されていない．

電子証明書の発行条件を表 2.2 に示す．

署名用電子証明書が 15 歳未満に対して発行しないのは，署名用電子証明書が実印に相当するものであるからである．

表 2.2: 電子証明書の発行条件.[11] を基に作成

| カード発行時の年齢 | 利用者証明用電子証明書 | 署名用電子証明書 |
|---|---|---|
| 20 歳以上 | 発行する | 発行する |
| 15 歳以上 20 歳未満 | 発行する | 発行する |
| 15 歳未満 | 発行する | 発行しない |

### 2.9.2　公的個人認証サービスにおける電子証明書の検証

電子証明書の署名検証の実施をする場面として，利用者が行政機関などに文書を提出した際に行政機関側が受け取った利用者の電子証明書の検証をする場面と行政機関から個人あてに返却された文書の電子証明書を検証する場面である．

利用者の電子証明書を検証が可能であるのは，電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（公的個人認証法）の第 17 条に記載されている，行政機関，裁判所と特定認証業務を行う民間事業者のうち内閣総理大臣や総務大臣による認定を受けた民間事業者である．電子証明書の失効条件は先述の通りである．失効しているかを確認する方法は 2 つある．

- CRL(Certificate Revocation List)
  認証局から定期的に証明書のシリアル番号とその証明書の失効情報 (有効期限よりも前に何らかの理由で失効したもの) のリストである CRL が配布され，それをダウンロードしてシリアル番号を照会して検証する．1 つの証明書を検証するためにも CRL 全体をダウンロードする必要がある．

- OCSP(Online Certificate Status Protocol)
  CRL の代替として策定されたものであり，OCSP レスポンダと呼ばれるサーバを稼働させ，そこで CRL を保管する．検証者は OCSP レスポンダに対して証明書のシリアル番号をもとに有効性の照会，署名付きの応答で有効性の検証を行う．電子証明書を個別に検証可能である．しかし，検証数が多くなると通信回数が多くなってしまう．

## 2.10　マイナンバーカード

マイナンバーカードとは，マイナンバーを保有する住民が申請すると無料で交付されるプラスチック製のカードであり，カード内に IC チップを搭載している．この IC チップ内に公的個人認証サービスで用いることができる電子証明書が搭載されており，公的な身分証明書としても利用できる IC カードである．マイナンバーカードの電子証明書の利用にはマイナンバーの使用はされていないため，番号法にふれることなく民間事業者を含めた様々な事業者が多様な用途に利用可能である．

マイナンバーカードの IC チップには 4 種類のカードアプリケーション (カード AP) が搭載されている．図 2.2 にマイナンバーカードの内部構成を示す．それぞれのカード AP の機能をまとめたものを表 2.3 に示す．

## 2.11　タイムスタンプ

タイムスタンプとは，デジタルデータがその日時において存在していたことを証明し (存在証明)，その日時以降にデータが変更されていないことを証明する技術である．タイムスタンプを発行してもらうにはタイムスタン

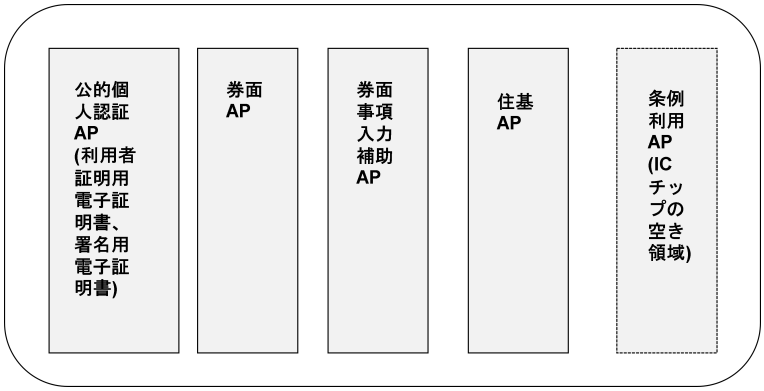


図 2.2: マイナンバーカードの AP 構成.[11] を基に作成

表 2.3: カード AP の機能.[11] を基に作成

| カード AP | 利用目的 | 暗証番号 |
|---|---|---|
| 公的個人認証 AP | 署名用電子証明書:電子申請に利用<br>利用者証明用電子証明書:マイナポータルのログインなどに利用 | 6~16 桁の英数字<br>4 桁の数字 |
| 券面 AP | 券面情報の改ざんの有無を検知 | - |
| 券面事項入力補助 AP | マイナンバーや基本 4 情報をテキストデータとして利用 | 4 桁の数字 |
| 住基 AP | 住民票コードの記録，テキストデータとして利用 | 4 桁の数字 |

プサービスの信頼の基盤でもある時刻認証局 (Time-Stamping Authority，以下「TSA」という) に特定のデータを送付する必要がある．送付するデータはメッセージダイジェストと呼ばれる，タイムスタンプを付与する元のデータのハッシュ値である．これを受け取った TSA はこのハッシュ値に時刻情報を偽造できないようにして結合したタイムスタンプトークンを送信者に送付することによりタイムスタンプを発行する．このときに付与されたタイムスタンプを検証するには TSA に送信した元のデータのハッシュ値を計算し，TSA により付与されたタイムスタンプに含まれているハッシュ値とを比較して，一致しているかを確認する．電子帳簿保存法においては電子取引の取引情報に係る電磁的記録の保存にタイムスタンプが付与されていることまたは受け取り後すぐにタイムスタンプを付すことが要件付けられているなど重要な意味を持つものである．

## 2.12 マルチシグネチャ

暗号資産を送金するためには，秘密鍵によりトランザクションに署名し，認証をする必要がある．その際，トランザクションの認証に複数の秘密鍵による署名を必要とする仕組みをマルチシグネチャ(以降マルチシグ) と呼ぶ．マルチシグの特徴として，単一の秘密鍵を用いて署名するシングルシグに比べて，高いセキュリティを実現できる，秘密鍵が紛失したときの対応が用意であるなどのメリットがある．しかし，全ての秘密鍵を別々の場所に保管する必要がある，複数の秘密鍵を利用するという複雑さがあるためコストがかかるといったデメリットがある．

N 個の秘密鍵のうち M 個の秘密鍵による署名により暗号資産の送金処理を可能にする場合，MofN のマルチシグと呼ぶ．2of3 マルチシグの例を図 2.3 に示す．

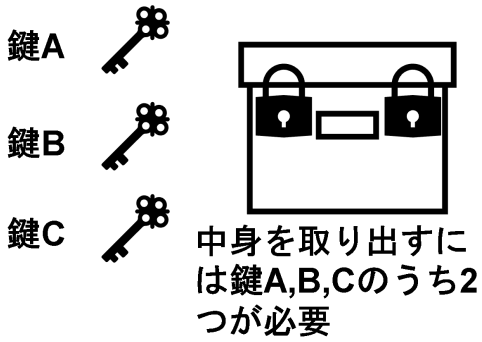


図 2.3: 2of3 マルチシグの例

# 第3章　公的個人認証サービスを利用したデジタル遺品相続サービス

## 3.1　相続を電子化する上での問題

デジタル遺品は，故人が利用していたオンラインサービスやデジタル機器に残されたデータである．機械的に処理を行うことにより，デジタル遺品の相続を完了させることができるのではないかと考える．しかし，現在のデジタル遺品の相続に対して故人ができることは，紙の遺言書にデジタル遺品へのアクセス方法及び処理方法を記載しておくことのみである．デジタル遺品の処理は，相続人に左右されてしまう．そこで本研究では，故人の意志が反映された遺言書をもとに機械的にデジタル遺品の相続を行うことにより，故人の意志を正確に反映した相続の実行できるシステムを提案する．デジタル遺品の種類は多く，すべてのデジタル遺品を相続対象とすることは困難である．そこで，本研究では，デジタル遺品の中でも，一般的なコミュニケーションツールとなった SNS アカウントと財産的な価値が認められ，相続税の対象にもなっている暗号資産に焦点を当てた．特に SNS アカウントは，死後のアカウント管理権限の設定を公式から提供されていない Twitter を，暗号資産は，世界初の暗号資産でもっとも有名な暗号資産である Bitcoin を本研究での相続対象とする．

相続を電子化する上での問題点として以下の 4 点を取り上げる．

- 遺言書の電子化
- 被相続人の死亡確認
- 相続人の本人確認性
- 送金処理を実施する際に発生する問題

### 3.1.1　遺言書の電子化

一般的に遺言書は日付及び氏名を自筆し，押印をすることが要件とされている．しかし，要件を満たした紙の遺言書をそのままスキャナで電子化したとしても有効な遺言書とは認められない．その理由としては，遺言書の筆跡や押印により真正性の証明を行うことができなくなっているからである．つまり，電子化した遺言書を有効にするためにはその真正性を第三者によって検証，確認できることが求められる．

### 3.1.2　被相続人の死亡確認

相続とは被相続人が亡くなった後に開始されるものであり，被相続人が生存している間は相続が発生してはいけない．電子的に死亡確認をする方法として一般的なものは存在しない．あるサービスを長期間利用していないことや SNS などによる死亡報告をもって死亡とするのは信憑性があまりにも乏しい．信頼できる機関である行政機関による報告などの信頼性のある確認が必要である．

### 3.1.3　相続人の本人確認性

相続人になりうる人物は基本的には親族であり，対面で相続を行う場合は相続人本人であることを確認することは容易である．しかし，電子的に行う場合，特に相続という重要な場面においての本人確認には強固な確認が必要となる．

### 3.1.4　送金処理を実施する際に発生する問題

通常，暗号資産はアドレスの管理者が保持しているアドレスに対応する秘密鍵を利用することで送金処理を完了することができる．しかし，暗号資産を相続するとなると管理者であった被相続人は死亡しているため，暗号資産の相続を行う際に被相続人が関与することはできない．暗号資産の相続を行うときに被相続人が保持していた秘密鍵を使用せずとも送金を可能にする必要がある．

## 3.2　問題解決に向けて

3.1 で述べた問題に対し，既存の技術及び制度で解決可能な問題を 3.2.1，3.2.2 に，既存の技術及び制度では解決できない問題を 3.2.3，3.2.4 に示す．

### 3.2.1　暗号資産の送金

暗号資産を相続するには，暗号資産の送金処理に必要となる秘密鍵を管理する必要がある．シングルシグ方式の場合，秘密鍵の管理者は被相続人であるため相続を行うには，被相続人の死後に秘密鍵の情報を相続人に譲渡する必要がある．しかし，被相続人の死後に秘密鍵の情報を相続人に譲渡するには，遺言書に残しておく必要がある．そうして残した場合，相続人以外の人物により盗み見られ暗号資産を不正に送金される危険がある．そこで，マルチシグの技術を利用する．自身の秘密鍵と共同署名者の公開鍵を利用することでマルチシグ対応アドレスを作成することができ，このアドレスに暗号資産を送金しておくことにより，被相続人の死後に被相続人の秘密鍵を使用せずとも暗号資産の相続を行うことができる．また，共同署名者を工夫することにより，特定の相続人による不正な送金処理を防ぐことができる．

### 3.2.2　本人確認

オンライン上での申請者の本人確認には，公的個人認証サービスを利用する．公的個人認証サービスで提供されている利用者証明用電子証明書を利用することにより，申請者の本人性確認が地方公共団体情報システム機構によって担保される．

### 3.2.3　遺言書の電子化

電子化された遺言書の有効性問題は，電子化された遺言書の真正性を証明することと遺言書の作成日時を特定できることにより解決される．遺言書に電子署名を付与することにより，遺言書作成者の証明と遺言書作成以降に遺言書が誰にも改ざんがなされていないことを検証できるため，遺言書の真正性の証明をすることができる．電

子署名の付与には，公的個人認証サービスで提供されている署名用電子証明書が利用できる．しかし，電子署名の付与だけでは，遺言書の作成日時を特定することはできない．

遺言書の作成日時を特定するためには，タイムスタンプを付与・検証する必要がある．しかし，公的個人認証サービスには，タイムスタンプを付与・検証できる仕組みは存在しないため，サービスの改正が必要となる．

### 3.2.4 死亡確認

死亡は，医師が書いた死亡診断書と死亡届を役所に提出，処理されることにより初めて受理される．その後，役所によって戸籍への記載や住民票の抹消手続きが行われる．公的個人認証サービスでは，この過程により住民票が抹消され戸籍に記されたことを信頼して電子証明書を失効させる．本研究では，公的個人認証サービスによる電子証明書の失効を検知することにより，遺言登録者の死亡を確認する．しかし，現状では失効させた電子証明書の失効理由に記載されるのは,「死亡」又は「海外転出」であるため，失効理由からでは電子証明書の所有者が本当に死亡したのかを検知することはできない．失効理由から「死亡」を検知できるシステムを導入する必要がある．

# 第4章　提案手法

## 4.1　システムの設計

相続関連業務は信託業務にあたるため，相続の執行人となる遺言書保管所は，信託業法第 3 条により内閣総理大臣の免許を受けた者でなければ営業することはできない．加えて，内閣総理大臣の免許を受けるためには，信託業法第 4 条に則った申請をする必要があるなど，法的規制も厳しい．営業の条件を満たしていたとしても遺言書保管所に相当な信頼がなければ，利用者は安心してサービスを利用することはできない．そのため，遺言書保管所には，法務省や法務局など相続関連業務を行う行政機関，もしくはすでに信託業務をしていて実績のある信託銀行により信頼性を担保されていることを証明するために官報や通知により URL などの案内をするという処置が必要である．

遺言書保管所に登録するための遺言書は，テンプレートを配布しておき，それに遺言を記入してもらうこととする．配布するテンプレートファイルの内容を図 4.1 に示す．遺言書のスキーマファイルを 4.2 に示す．

本提案手法では遺言書に記載する暗号資産のアドレスをもつ 2of4 のマルチシグウォレットは遺言書保管所と登録者の相互やり取りで作成する．ウォレットとアドレスを作成するために，登録者は自身が保持している公開鍵を実装プログラムに送信する．実装プログラムは，登録者より受信した公開鍵と遺言書保管所の鍵を用いて相続に利用するためのウォレットとアドレスを作成する．その後，実装プログラムは作成したアドレスとウォレット作成に利用した遺言書保管所の公開鍵を登録者に返送する．返送されたアドレスが相続に利用するアドレスとなる．遺留分によるトラブルを防ぐために登録者はそのアドレスに対し，相続人の遺留分以上の額の暗号資産を送金しておくものとする．

秘密鍵は遺言書保管所が 2 つ，登録者が 1 つ，そして，登録者の相続人が 1 つ保持しているとする．また，相続人が 2 人以上いる場合は相続人の人数分のウォレットを作成しているものとする．登録者が秘密鍵を保持する理由は，登録者の死亡前は暗号資産は登録者の財産であり，それを証明するためにも秘密鍵の保持が必要となるからである．相続人が秘密鍵を 1 つ (半数未満) 保持するのは，相続発生時に秘密鍵を保持していることによる認証を行うためである．加えて，相続人単体では送金処理を防止するためでもある．遺言書保管所が秘密鍵を 2 つ (半数以上) 保持するのは，相続発生時に相続人の秘密鍵紛失など，何らかの問題で送金処理ができなくなってしまうことを防止するためである．

さらに，本研究で相続対象としているものである Twitter アカウントについても事前に登録してもらう必要がある．ただし，Twitter アカウントのログイン情報である ID やパスワードを登録するのではなく，Twitter API によって選択をすることができる権限を選択して登録してもらうというものである．ログイン情報を遺言書に記載してしまうと，遺言書登録以降にパスワードの変更が容易にできなくなってしまう．遺言書を他人に盗聴された場合，登録者が認知しないうちに不正アクセスによるなりすましがされてしまうリスクが生じるからである．また，権限を設定しておくことで自身の死後に見られたくない情報へのアクセスを防ぐ配慮の目的がある．

以上を終えた後，登録者は遺言書保管所に自身の遺言書を登録してもらうための準備を行う．登録者が遺言書を保管所に登録するための事前準備の構成図を図 4.3 に示す．

```
<?xml version="1.0" encoding="UTF-8"?>↓
<Will↓
xmlns="http://www.w3schools.com"↓
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"↓
xsi:schemaLocation="http://www.w3schools.com template.xsd">↓
    <!--遺言者本人氏名-->↓
    <Author>↓
        <Fullname>TanakaTarou</Fullname> ↓
        <number>999999999999</number>↓
    </Author>↓
    <Declear>私は本遺言書により以下の通りに遺言する。</Declear>↓
    <!--Contentsには各相続人に向けて相続対象のアドレスを指定-->↓
    <Contents>↓
        <sentence>11111111111に以下の暗号資産を取得させる</sentence>↓
        <tonum>11111111111</tonum>↓
        <crypto_currency>**********************</crypto_currency>↓
    </Contents>↓
     <Contents>↓
        <sentence>222222222222に以下の暗号資産を取得させる</sentence>↓
        <tonum>222222222222</tonum>↓
        <crypto_currency>**********************</crypto_currency>↓
    </Contents>↓
    <Contents>↓
        <sentence>333333333333に以下の暗号資産を取得させる</sentence>↓
        <tonum>333333333333</tonum>↓
        <crypto_currency>**********************</crypto_currency>↓
    </Contents>↓
    <!--オプション-->↓
    <Option>↓
    <!--sentenceには暗号資産を受け取らなかった場合のことや↓
    Twitterアカウントに関することを記載-->↓
        <sentence>以下のアカウントをお願いする</sentence>↓
        <!--Twitterアカウントの指定(今回は必須に指定)-->↓
        <twitter_ID>AccounttoDevel1</twitter_ID> ↓
    </Option>↓
</Will>↓
```

図 4.1: 遺言書テンプレート

## 4.2 遺言書登録

遺言書には「自筆証書遺言」を利用する．理由は，公正証書遺言や秘密証書遺言は作成のために手間や費用がかかることや作成時に立会人や法定証人の二人以上の参加が必要になるなど電子的に手続きを行うための障害になるからである．しかし,「自筆証書遺言」では内容が適切に書けていたとしても形式に不備がある場合には無効な遺言書とされてしまう．登録者のミスにより遺言書の形式が崩れてしまい遺言書自体が無効になってしまう恐れがあるため，遺言書登録時に有効な遺言書の形式であるかを確認する必要がある．登録者が遺言書を保管所に登録する際の構成図を図 4.4 に示す．

遺言書登録後に，遺言書保管所は，登録者の署名用電子証明書の発行番号を地方公共団体情報システム機構の電子証明書の紐付け情報データベースに送信する．遺言書保管所は，登録者の利用者証明用電子証明書の発行番号を回答として受け取り，その情報を電子証明書と関連付けて保管する．受け取った情報は登録者の死亡確認処理に利用される．

```
<?xml version="1.0" encoding ="utf-8"?>
    <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    targetNamespace="http://www.w3schools.com"
    xmlns="http://www.w3schools.com"
    elementFormDefault="qualified">
        <xsd:element name="Will">
            <xsd:complexType>
                <xsd:sequence>
                    <xsd:element ref="Author"/>
                    <xsd:element name="Declear" type="xsd:string"/>
                    <xsd:element ref="Contents" minOccurs="1" maxOccurs="unbounded"/>
                    <xsd:element ref="Option" minOccurs="0" maxOccurs="1"/>
                </xsd:sequence>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="Author">
            <xsd:complexType>
                <xsd:sequence>
                    <xsd:element name="Fullname" type="xsd:string" minOccurs="1" maxOccurs="1"/>
                    <xsd:element name="number" type="xsd:string" minOccurs="1" maxOccurs="1"/>
                </xsd:sequence>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="Contents">
            <xsd:complexType>
                <xsd:sequence>
                    <xsd:element name="sentence" type="xsd:string" minOccurs="1" maxOccurs="1"/>
                    <xsd:element name="tonum" type="xsd:string" minOccurs="1" maxOccurs="1"/>
                    <xsd:element name="crypto_currency" type="xsd:string"  minOccurs="1" maxOccurs="1"/>
                </xsd:sequence>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="Option">
            <xsd:complexType>
                <xsd:sequence>
                    <xsd:element name="sentence" type="xsd:string" minOccurs="1" maxOccurs="1"/>
                    <xsd:element name="twitter_ID" type="xsd:string" minOccurs="1" maxOccurs="1"/>
                </xsd:sequence>
            </xsd:complexType>
        </xsd:element>
    </xsd:schema>
```

図 4.2: 遺言書のスキーマファイル

## 4.3　死亡確認方法

遺言書保管所による被相続人の死亡確認には，マイナンバーカードの利用者証明用電子証明書の失効およびその失効理由を利用する．利用者証明用電子証明書の失効条件は，2.9.1 節で述べたように署名用電子証明書よりも少ないからである．しかし，表 4.1 に示した現在の公的個人認証サービスの電子証明書の失効理由では,「死亡」のみを確実に検知することができない．

表 4.1: 電子証明書失効理由.[12] を基に作成.

| 失効理由 | 判断できること |
|---|---|
| affliationChanged | 「死亡」または「海外転出」 |
| cessationOfOperation | 「カード紛失」または「海外転出」 |
| Superseded | 「証明書更新」 |
| certificateHold | 「カード紛失」 |

そこで，本研究で新たに導入する公的個人認証サービスの除票を用いた検証により，登録者の死亡確認行う．除票は地方公共団体情報システム機構により 24 時間ごとに発行されるものとする．ただし，除票にアクセスもしくはダウンロードが可能なのは，現行の公的個人認証サービスの CRL と同様に署名検証者または団体署名検証者のみとする．遺言書保管所は署名検証者または団体署名検証者であるとする．

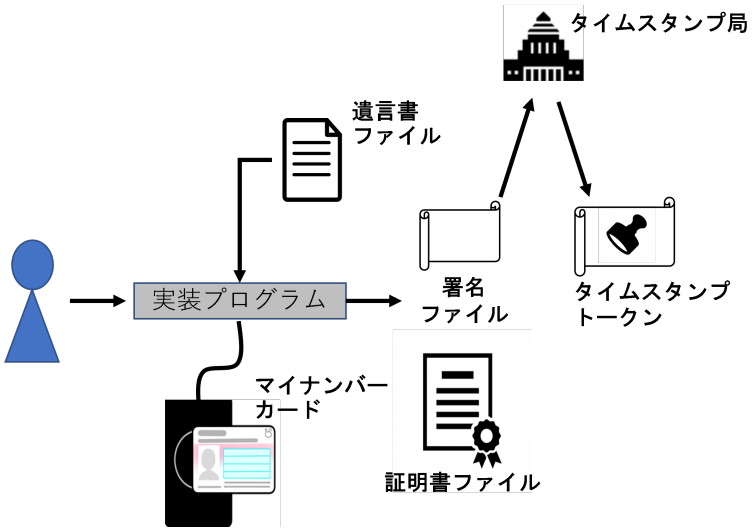


図 4.3: 事前準備

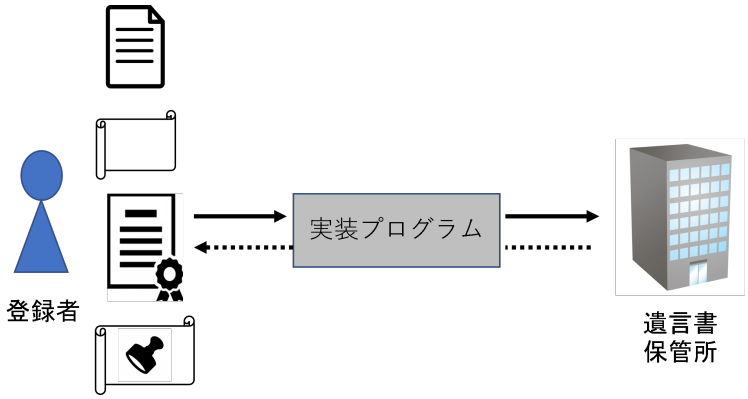


図 4.4: 遺言登録

## 4.4 相続方法

相続は遺言保管所により，登録者の死亡確認が完了した後にのみ実行される処理である．例え相続人からの申請があったとしても被相続人の死亡確認処理が完了していない場合には処理されるべきではない．

相続を行う相手は遺言書に記載されている相続人である必要があるため，相続処理を行う際には相続人の認証を行う．相続人の認証には，マイナンバーカードの利用者証明用電子証明書による本人認証を用いる．これは，コンビニエンスストアでの住民票交付など証明書の交付が受けられるサービスでも利用されている方法でもある．これを用いることにより，公的個人認証サービスによる信頼性のある認証をすることができるほか，その際に取得したマイナンバーを利用することで相続の申請を行った相続人を識別することができる．

相続人の認証が完了したのち，遺言書に記載されている相続人毎の遺言の内容に応じた手続きを実行する．本研究で相続対象となるデジタル遺品は，Bitcoin と Twitter アカウントの操作権限である．

ここで，遺言書に記載されたアドレスには，各相続人の属性に応じた遺留分額以上の暗号資産が被相続人により入金されている，入金後はそのアドレスからの送金処理は，相続が実行されるより前には行われないという 2 つ

の前提条件を設ける．

Twitter アカウントの操作権限を設定する，権限に基づいた操作を実行するために公式から提供されている Twitter API を実装に用いる．

# 第5章　実装

## 5.1　遺言書登録処理

マイナンバーカードの電子証明書を利用した署名は，カードへ送信したデータをカード内の秘密鍵で暗号化し返送しているだけであり，カード外へ秘密鍵を取り出すことは不可能になっている．IC カードと IC カードリーダ間の通信をするための規格である APDU(Application Protocol Data Unit)[13] コマンドをマイナンバーカードに送信することで電子署名を実現する．署名アルゴリズムには sha256RSA が使用されており，公開鍵は証明書の中に含まれているため証明書ファイルも取り出している．この操作を可能にするには，マイナンバーカードを取得する際に登録したパスワードが必要であるため，パスワードが漏洩していない限りは自身のマイナンバーカードを使用して他人が遺言書に署名を付すことはできなくなっている．

本実装で行っているのは署名用電子証明書の秘密鍵を用いた電子署名である．マイナンバーカードを用いた電子署名では電子申請の際に文書の作成者を証明するためには署名用電子証明書を用いることが一般的であることや 15 歳未満には実印に相当する署名用電子証明書の発行は行われないためである．加えて，民法第 961 条により遺言をするための意思能力は 15 歳になってからであることも理由の一つである．

登録者は実装プログラムに対し，図 4.3 に示した事前準備で作成したファイル群を実装プログラムを通して送信する．遺言書は xml 形式で作成されており，保管所側は遺言書の登録を済ませる前に XML Schema による検証，遺言書の署名の検証，タイムスタンプの検証の 3 つによって遺言書の形式確認を行う．本システムでアップロードするファイルは，以下の 4 点である．

- **遺言書**
  登録したい遺言書ファイル本体である．
- **署名付き遺言書**
  署名用電子証明書の秘密鍵で署名された遺言書ファイルであり，遺言書の非改ざん証明に使用される．
- **署名用電子証明書**
  本人性確認と公開鍵を取り出し署名検証をするために使用される．
- **タイムスタンプトークン**
  遺言書の存在証明と非改ざん証明に使用される．

実装プログラムは，遺言保管所に遺言書を登録する前に送信された遺言書が正しいものであるかを判定する．遺言書が正しいものであるとは，登録者である被相続人が遺言能力を有している，形式的に正しい遺言書であるという 2 つの要件を満たしているものである．遺言能力を有していることを確認するためには民法第 961 条より，満 15 歳以上である必要がある．さらに，正常な判断能力を有している必要があるがそれについての明確な定義が存在しない．そのため，遺言書の登録者が満 15 歳以上であること，形式的に正しい遺言書である，という 2 つをもって正しい遺言書であるとする．

事前準備のための実装プログラムでは，マイナンバーカードの署名用電子証明書による署名を実行した．しかし，マイナンバーカードを用いた署名方法には利用者証明用電子証明書を用いるものも存在する．利用者証明用電子証明書は 15 歳未満の者であっても発行されるため，電子署名を検証するだけではその署名に用いられた証明書が署名用電子証明書であるのか利用者証明用電子証明書であるのかが確認できず，登録者が満 15 歳以上であることが確認できない．そこで，まず実装プログラムは，アップロードされた電子証明書が署名用電子証明書であることを確認する．

次に，実装プログラムが行うことは，XML Schema による遺言書ファイルの検証である．XML Schema による確認により，遺言書のテンプレートをもとに作成されたものであることの検証を行うことで，本来想定している遺言書と全く関係のないファイルの誤登録を防ぐことができる．

その後，実装プログラムは，遺言書の署名・タイムスタンプトークンの検証を行う．遺言書の署名を受信した署名用電子証明書の公開鍵を用いて検証することで，遺言書の真正性を確認する．また，タイムスタンプトークンの検証をすることにより遺言書作成日の特定やタイムスタンプが付与された以降に改変されていないことを二重に確認する．

遺言書が登録されると，遺言書保管所側から登録者に遺言書の「預り証」を発行する．預り証には，登録された内容物と登録者名，登録を受けた日付，預り証の発行機関名，預り証番号が記載されている．その預り証に遺言書保管所による電子署名とタイムスタンプを付与したものを登録者に返送する．遺言書登録以降の処理に，この預り証を用いることで円滑に手続きを進めることができる．

実際の実行例を図 5.1 に，実行後遺言保管所より返送された預り証を図 5.2 に示す．実行時のフローチャートを図 5.3 に示す．


図 5.1: 登録処理実行例


図 5.2: 返送された預り証

## 5.2　死亡確認処理

遺言書保管所による登録者の死亡確認には，本研究で作成した除票を用いる．登録者の利用者証明用電子証明書の失効理由が「死亡」と記されている場合にのみ，遺言書保管所による登録者の死亡確認が完了したものとす

る．図 5.4 に示した死亡確認処理の動作手順は，次の通りである．
① 遺言書保管所は登録者の利用者証明用電子証明書の失効確認を実装プログラムに要求する．
② 実装プログラムは地方公共団体情報システム機構により発行された除票にアクセス，ダウンロードをする．
③ 実装プログラムは利用者証明用電子証明書の失効確認の結果，失効しているならその理由を遺言書保管所に通知する．
本研究で作成した除票を図 5.5 に，除票のスキーマファイルを図 5.6 示す．

## 5.3 相続処理

相続処理は遺言保管所による死亡確認処理が完了した後にのみ実行される処理である．例え相続人から申請があったとしても，被相続人の死亡確認処理が完了していない場合には処理されるべきではない．

相続処理を実行するために，実装プログラムは相続人を識別し，認証する．しかし，公的個人認証サービスによる認証の機能が搭載されたプログラムの作成は，情報連携するための API が公開されておらず，実装することができなかった．そのため，マイナンバーカードからマイナンバーを取りだし，相続人の識別のみを行うプログラムとなっている．

Bitcoin の相続手続きでは，相続人の識別後，遺言書に記載されているアドレスを公開する．その後，相続人が所持している秘密鍵を用いて，相続手続きにより公開されたアドレスから送金処理を実行するために署名をする．相続人により署名されたことを遺言書保管所が確認したのちに，遺言書保管所による署名を行うことで送金が完了する．

Twitter アカウントの相続手続きは，故人によって登録された操作権限に基づいた処理のみ実行できるものとした．しかし，Twitter API によって選択できるのは，読み込み，読み込みと書き込み，読み込みと書き込みとダイレクトメッセージの閲覧と送信，という 3 つの権限レベルのみである．データ単位での設定や書き込みのみを許可する権限の設定はできない．Twitter API の仕様上，相続人が行う権限に基づいた操作回数には 15 分間に 15 回などの制限がある．

## 5.4 開発環境

本システムは表 5.1 に示す開発環境で開発された．相続に利用するマルチシグウォレットおよびアドレスの作成は python のライブラリである bitcoinlib[14] を利用した．相続する Twitter アカウントの権限設定のための Twitter API を操作するために php のライブラリである twitteroauth[15] を使用した．マイナンバーカードとの通信には，Python ライブラリの pyscard[16] で提供されている機能を使用した．署名・証明書の検証などの暗号化関数の利用には，OpenSSL[17] を用いた．

表 5.1: 開発環境.

| ハードウェア・ソフトウェア | 環境 | バージョン |
|---|---|---|
| カードリーダー | SMART ATM CARD READER | - |
| 暗号資産ライブラリ | bitcoinlib | 0.6.3 |
| Twitter API ライブラリ | twitteroauth | 3.1.0 |
| スマートカードライブラリ | pyscard | 2.0.2 |
| 暗号ライブラリ | OpenSSL | 1.1.1k |

## 5.5　評価

遺言書を登録するために，既存の技術である公的個人認証サービスの署名用電子証明書を利用して，遺言書に署名を付与するプログラムを新たに実装した．これにより電子署名を検証することが可能になり，遺言書の真正性を確かめることができるようになった．また，公的個人認証サービスにタイムスタンプを付与する仕組みが増設されたという前提をもとに実装したことにより，ある時刻以降における遺言書の存在証明することができた．一方で，遺言書登録時点で証明書が失効していると，電子署名による本人証明や非改ざん証明が意味をなさなくなるため，署名用電子証明書の有効性を検証する必要がある．しかし，公的個人認証サービスの情報連携 API が一般公開されていないため署名用電子証明書の有効性を検証することができない実装となった．

現在の公的個人認証サービスには，死亡確認を行うことができるシステムが存在しない．公的個人認証サービスで死亡確認を実現するために，新たに除票とそのスキーマファイルを定義し導入した．これにより，利用者証明用電子証明書のシリアル番号を基にした電子証明書の失効理由を確認することで，信頼性のある利用者の死亡確認をオンライン上で行うことが可能となった．

公的個人認証サービスを用いた利用者証明用電子証明書による本人認証が利用でき，相続人が正しく認証されたことを前提として，デジタル遺品の相続処理を行うプログラムを実装した．実装プログラムにより，本研究で相続の対象とした Twitter アカウントの操作権の相続を行うことができるようになった．また，本研究のもう一つの相続対象であるビットコインの相続については，遺言書に登録されたアドレスを対象の相続人に公開するまでは実装できた．しかし，時間の都合上，実際に送金処理を実行するプログラムを実装することはできなかった．

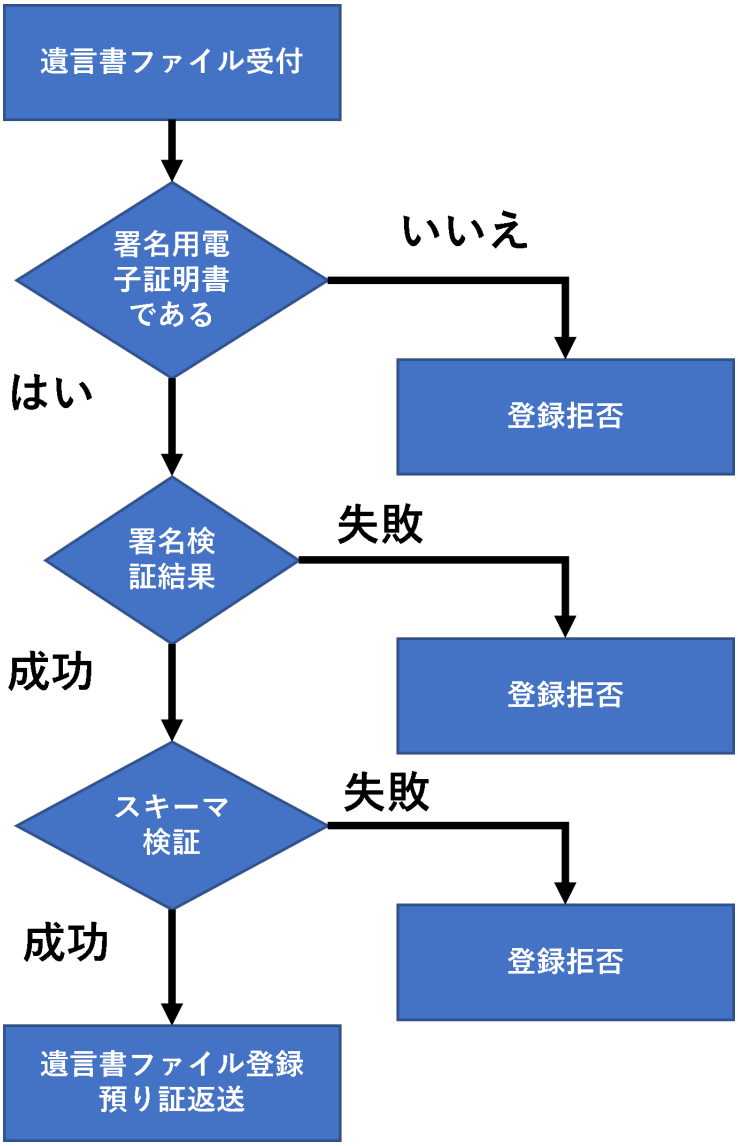


図 5.3: 登録処理のフローチャート

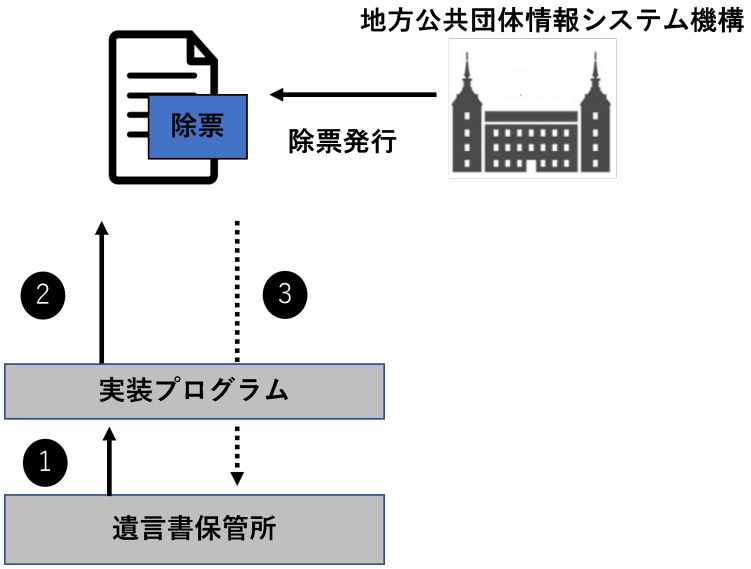


図 5.4: 死亡確認処理

```
<?xml version="1.0" encoding="UTF-8"?>↓
    <deleted_residence_record↓
    xmlns="http://www.w3schools.com"↓
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"↓
    xsi:schemaLocation="http://www.w3schools.com deleted_residence_record.xsd">↓
        <Title>除票</Title>↓
        <Date_of_issue>20220105</Date_of_issue>↓
        <Next_date_of_issue>20220106</Next_date_of_issue>↓
        <Certificates>↓
            <serial_number>029509a2</serial_number>↓
            <expire_date>20211231</expire_date>↓
            <!--死亡,海外転出-->↓
            <reason>死亡</reason>↓
        </Certificates>↓
        <Certificates>↓
            <serial_number>99999999</serial_number>↓
            <expire_date>20220101</expire_date>↓
            <!--死亡,海外転出-->↓
            <reason>海外転出</reason>↓
        </Certificates>↓
        <End>0</End>↓
    </deleted_residence_record>↓
←
```

図 5.5: 除票

```
<?xml version="1.0" encoding ="utf-8"?>↓
    <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"↓
    targetNamespace="http://www.w3schools.com"↓
    xmlns="http://www.w3schools.com"↓
    elementFormDefault="qualified">↓
    ↓
        <xsd:element name="Deposit">↓
            <xsd:complexType>↓
                <xsd:sequence>↓
                    <xsd:element name="Title" type="xsd:string"/>↓
                    <xsd:element name="Date_of_issue" type="xsd:string"/>↓
                    <xsd:element name="Next_date_of_issue" type="xsd:string"/>↓
                    <xsd:element ref="Certificates"/>↓
                    <xsd:element name="End" type="xsd:string"/>↓
                </xsd:sequence>↓
            </xsd:complexType>↓
        </xsd:element>↓
            ↓
        <xsd:element name="Certificates" maxOccurs="unbounded">↓
            <xsd:complexType>↓
                <xsd:sequence>↓
                    <xsd:element name="serial_number" type="xsd:string" minOccurs="1" maxOccurs="1"/>↓
                    <xsd:element name="expire_date" type="xsd:string" minOccurs="1" maxOccurs="1"/>↓
                    <xsd:element name="reason" type="xsd:string" minOccurs="1" maxOccurs="1"/>
                </xsd:sequence>↓
            </xsd:complexType>↓
        </xsd:element>↓
↓
    </xsd:schema>←
```

図 5.6: 除票のスキーマファイル

# 第6章　結論

## 6.1　本研究のまとめ

本研究では，デジタル遺品の処理にともなうトラブルに着目し，相続の電子化を目標に設定した．問題解決のアプローチとして，遺言書の電子化とそれに付随した相続のオンライン化とその手法について提案した．

提案手法では，遺言書の電子化へのアプローチとして，元来自筆が要件とされている自筆証書遺言をもとに，XML Schema による遺言書の形式確認，遺言書の真正性の担保をするために，遺言書をマイナンバーカードに搭載される署名用電子証明書の秘密鍵で署名し，署名時に利用した証明書とともに登録した．また，遺言書にタイムスタンプを付与，検証可能な状態で公開することにより，遺言書作成日時以降の非改ざん証明をすることに成功した．

また，提案手法では，公的個人認証サービスに除票を導入し，細分化した証明書の失効理由をもとに死亡確認を実施することにより，オンライン上でも厳格で信頼性のある死亡確認を実現することを可能にすることを示した．

本提案手法をもとにした実装をすることで，相続人を識別し，デジタル遺品の相続をオンラインで機械的な実行を可能にすることを示した．

## 6.2　本研究の課題

本研究では，被相続人や相続人の識別のためにマイナンバーを利用した．しかし実際には，被相続人や相続人の認証は地方公共団体情報システム機構によるものでありマイナンバーは識別のための情報に過ぎない．マイナンバーは「マイナンバー法」により定められた社会保障，税，災害対策の手続き以外で利用することができない．そのため，マイナンバーなどの法的な制約を受けるものとは異なり，相続人の識別情報として個人を識別することが可能である情報を利用することが必要である．

相続人一人一人に対して 2of4 のウォレットを作成しているため，相続人の数が多ければその分遺言書保管所によるウォレットの管理コストが大きくなるという問題がある．また，2of4 のマルチシグウォレットのうち 2 つの秘密鍵は遺言書保管所により管理されているため遺言書保管所と相続人との共謀もしくは，遺言書保管所単体で不正に暗号資産を送金できてしまう．しかし，遺言書保管所が過半数の鍵を所持しておかなければ相続人が鍵を紛失してしまったしたときに暗号資産があるにもかかわらず送金処理ができなくなってしまう．マルチシグの特性を上手く利用し必要鍵数や鍵の管理人を増やす，鍵の分配方法を調整することで，不正送金を防ぎながら一人当たりの鍵管理コストを削減する方法を検討する必要がある．

被相続人の死亡後に開始された相続において，相続が完了する前に相続人 (A とする) が亡くなってしまった場合，遺留分を含めた相続可能な割合は変化しないため，A 以外の相続人には問題なく相続が可能である．しかし，通常であれば A の相続人に遺産が渡るべきである (数次相続の発生)．本提案手法では，A が遺言書を登録していない場合，本来 A の相続人に相続されるべき遺産の送金処理自体は可能であるが A の相続人を知ること，またその証明ができないために送金できないという問題が発生する可能性があるため，これに対応する方法について検討する必要がある．

## 6.3 本研究の展望

本研究では，遺言書を電子化するための要件として，遺言書の真正性を第三者により証明できるものとした．しかし，現行の民法では，本研究の要件を満たしたとしても遺言書の有効性が認められるわけではない．財産目録の自書が不要と改正されたように，遺言書の「自書」が不要となるように改正される必要がある．

本研究では限定したデジタル遺品相続にのみ注目したものであるが，実際に相続を行う際はデジタル遺品のみでなく普通の遺産の相続が伴うことがふつうである．本研究で示した遺言書の電子化とそれに付随したサービスを用いることでデジタル遺品のみならず，普通の相続も電子的に完結させることが可能になる．

マイナンバー単体では悪用することはできないにもかかわらず，たとえ本人の許可があろうともマイナンバーを公開することは認められていない．また，マイナンバーは隠すものであるという印象はマイナンバーの活用を妨げていると推測できるためマイナンバーの秘匿を不要にする，もしくは，本人の許可があればマイナンバーの使用を認めるというようにすれば様々な場面で活用可能になると考える．マイナンバーカードやその電子証明書の仕様が一般に公開されていない．そのため，これらを活用したサービスを展開することは困難である．これらを公開することで様々なサービスや制度の基盤となる．

# 謝辞

本研究を行うにあたり，研究の着想から，論文執筆まで多くの助言，ご指導をしてくださいました上原哲太郎教授に心より感謝申し上げます．また，サイバーセキュリティ研究室の皆様をはじめ，本研究を行う上で支えてくださったすべての方々に感謝申し上げます．

# 参考文献


[1] 総務省. 令和 2 年通信利用動向調査. https://www.soumu.go.jp/johotsusintokei/statistics/data/210618_1.pdf. 閲覧日:2021-12-19.

[2] 亡くなられた利用者のアカウントについてのご連絡. https://help.twitter.com/ja/rules-and-policies/contact-twitter-about-a-deceased-family-members-account. 閲覧日:2021-11-3.

[3] 自筆証書遺言書保管制度のご案内. https://houmukyoku.moj.go.jp/mito/page000001_00041.pdf. 閲覧日:2021-11-25.

[4] 中川善之助, 泉久雄. 相続法第 4 版.pp.514-527. 有斐閣社,2000.

[5] 最高裁判所判決平成元年 2 月 16 日民集　第 43 巻 2 号 45 頁. https://www.courts.go.jp/app/hanrei_jp/detail2?id=52210. 閲覧日:2021-12-30.

[6] 東京高等裁判所昭和 62 年 5 月 27 日第 40 巻 1 号 38 頁. https://www.courts.go.jp/app/hanrei_jp/detail2?id=020310. 閲覧日:2021-12-30.

[7] 最高裁判所判決平成 28 年 6 月 3 日民集　第 70 巻 5 号 1263 頁. https://www.courts.go.jp/app/hanrei_jp/detail2?id=085930. 閲覧日:2021-12-30.

[8] 総務省. 公的個人認証サービス利用のための民間事業向けガイドライン. https://www.soumu.go.jp/main_content/000400619.pdf. 閲覧日:2021-10-2.

[9] 総務省. 主務大臣認定事業者. https://www.soumu.go.jp/main_content/000747198.pdf. 閲覧日:2022-1-15.

[10] 地方公共団体情報システム機構. 公的個人認証サービスポータルサイト. https://www.jpki.go.jp/procedure/period.html. 閲覧日:2021-10-2.

[11] マイナンバー制度とマイナンバーカード. https://www.soumu.go.jp/kojinbango_card/03.html. 閲覧日:2021-10-21.

[12] 本人確認のデジタル化・厳格化の推進について. https://www.nichigosho.net/topics/images/20200227.pdf. 閲覧日:2021-10-2.

[13] 密着型 IC カードの実装規約 第 4 章. https://www.nmda.or.jp/nmda/ic-card/iso10536/sec4.html.

[14] bitcoinlib. https://github.com/1200wd/bitcoinlib. 閲覧日:2021-12-21.

[15] TwitterOAuth. https://github.com/abraham/twitteroauth. 閲覧日:2021-10-19.

[16] pyscard. https://github.com/LudovicRousseau/pyscard. 閲覧日:2021-10-2.

[17] OpenSSL. https://www.openssl.org. 閲覧日:2021-10-2.

[18] 公的個人認証サービス (電子証明書) 中央区ホームページ. https://www.city.chuo.lg.jp/smph/kurasi/toroku/koutekikozinnninnsyuou.html. 閲覧日:2022-1-15.